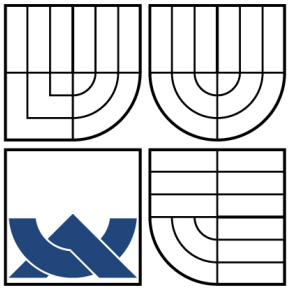
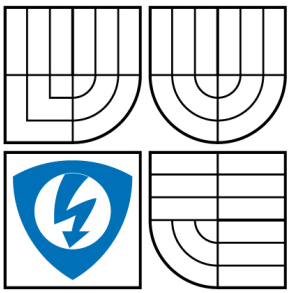


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

VODOZNAČENÍ STATICKÝCH OBRAZŮ

WATERMARKING OF STATIC IMAGES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. PETR BAMBUCH
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR ČÍKA
SUPERVISOR

BRNO 2008

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bambuch Petr Bc.	***ID:***	54459
Ročník:	2	***Akademický rok:***	2007/2008

NÁZEV TÉMATU:

Vodoznačení statických obrazů

POKYNY PRO VYPRACOVÁNÍ:

Podrobně prostudujte současné techniky pro vodoznačení statického obrazu. Navrhněte alespoň dvě metody vkládající do obrazu vodoznak. Pro ověření navržených metod použijte MATLAB. Vytvořené metody porovnejte pomocí dostupných aplikací Stirmark, Optimark, nebo CheckMark, které vodoznaky hodnotí .

DOPORUČENÁ LITERATURA:

[1] CHUN-SHIEN, L. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Hershey: Idea Group Publishing, 2004. ISBN: 1-59140-275-1
[2] ARNOLD, M., SCHMUCKER, M., WOLTHUSEN, D. S. Techniques and Applications of Digital Watermarking and Content Protection. Boston: Artech House Publishers, 2003. ISBN: 1-58053-111-3

Termín zadání:	11.2.2008	***Termín odevzdání:***	28.5.2008

Vedoucí práce: Ing. Petr Číka

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práve třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bc. Petr Bambuch
Bytem: Nová čtvrť 228, 75701, Valašské Meziříčí - Poličná
Narozen/a (datum a místo): 3.3.1984, Valašské Meziříčí

(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií
se sídlem Údolní 244/53, 60200 Brno 2
jejímž jménem jedná na základě písemného pověření děkanem fakulty:
prof. Ing. Kamil Vrba, CSc.

(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☑ diplomová práce
   - ☐ bakalářská práce

   jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP: Vodoznačení statických obrazů
Vedoucí/školitel VŠKP: Ing. Petr Číka
Ústav: Ústav telekomunikací
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

- ☑ tištěné formě - počet exemplářů 1
- ☑ elektronické formě - počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2

Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3

Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

ABSTRAKT

Diplomová práce se zabývá problematikou zabezpečení statických obrazů. Jde o přidání tajné informace k informačnímu obsahu obrazu, tak aby nebylo možné vložený vodoznak odstranit jednoduchými postupy. Spolu s vývojem techniky vodoznačení se zdokonaluje a rozvíjí technika útoků. Jejím cílem je odstranění, znehodnocení vloženého vodoznaku. Práce si klade za cíl prostudovat současné techniky vodoznační statického obrazu a na dvou zrealizovaných metodách vodoznačení ověřit jejich odolnost proti jednotlivým útokům.

KLÍČOVÁ SLOVA

vodoznačení, vodoznak, obraz, DCT, podvzorkování, útoky, Checkmark, Matlab

ABSTRACT

The thesis deals with the security of static images. The main aim is to embed the watermark into the original data so effectively, to avoid removal of the watermark with the use of simple and fast attacks methods. With developing of the watermarking techniques the technique of attacks are improved and developed also. The main aim of the attacks is to remove and devalue the hidden watermark in the image. The goal of the thesis is to check current techniques of static image watermarking and implement two methods of watermarking, which are to be tested for robustness against attacks.

KEYWORDS

watermarking, watermark, image, DCT, subsampling, attacks, Checkmark, Matlab

BAMBUCH, P. *Vodoznačení statických obrazů.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 54 s. Vedoucí diplomové práce Ing. Petr Číka.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Vodoznačení statických obrazů“ jsem vypracoval samostatně pod vedením svého vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne …… ……..

(podpis autora)

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucímu diplomové práce panu Ing. Petru Číkovi za ochotu, vstřícné jednání a za užitečnou metodickou pomoc.

V Brně dne …… ……..
(podpis autora)

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

DCT (discrete cosine transform) – diskrétní kosinová transformace

DWT (discrete wavelet transform) – diskrétní vlnková trnasformace

HVS (human visual system) – lidský vizuální systém

JPEG (joint photographic experts group) – formát komprese obrazu

LSB (least significant bit) – metoda vodoznačení v obrazové oblasti

MAE (mean absolute error) – střední absolutní chyba

MSE (mean square error) – střední kvadratická chyba

NCC (normalized cross-correlation) – normalizovaná vzájemná korelace

PSNR (peak signal-to-noise ratio) – špičková hodnota signál-šum

RGB (red green blue) – barevný model

SNR (signal-to-noise ratio) – odstup signál-šum

XOR (exclusive OR) – logická funkce

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době je velkým trendem uchovávat data v digitální podobě. Ať už se jedná o obrazovou, zvukovou ale i textovou podobu, je potřeba tato data nějakým způsobem chránit. Typickou ochranou za účelem prokázání vlastnictví je použití digitálních vodoznaků.

Diplomová práce je zaměřena na digitální vodoznačení statických obrazů. Úvod je věnován charakteristice vodoznaků a požadavkům kladeným na efektivní zabezpečení obrazových dat. Druhá část obsahuje popis dostupně veřejných aplikačních nástrojů, sloužících k testování odolnosti a hodnocení vodoznačení. Zaměření je na aplikační nástroj Checkmark. Poslední část obsahuje popis, realizaci a testování metod vodoznačení ve frekvenční oblasti. Aplikace na vložení vodoznaků a jejich detekci v obraze byly zrealizovány v prostředí MATLAB s podporou knihovny pro zpracování obrazu (Image Processing Toolbox).

1. Digitální vodoznaky

Historie digitálních vodoznaků je poměrně krátká záležitost. Tato technika, používaná k ochraně vlastnických práv, se zrodila počátkem devadesátých let 20. století. Je založena na principu [2] vkládání digitálního vodoznaku do nechráněného digitálního obsahu (např. do obrazových, zvukových a video dat). Při podezření na porušení autorského práva je vložený vodoznak z chráněných dat vytažen, aby jednoznačně dokázal vlastnictví autora. Důležitou vlastností vodoznaků je odolnost proti úmyslné či neúmyslné modifikaci vodoznačeného digitálního obsahu.

V dnešní době, spolu s vývojem techniky vodoznačení, se také rozvíjí a zdokonalují útoky, vedoucí k odstranění vloženého vodoznaku.

1.1. Základní pojmy

Vodoznak: Je viditelná nebo skrytá obrazová informace (např. logo), posloupnost symbolů i jednobitová informace.

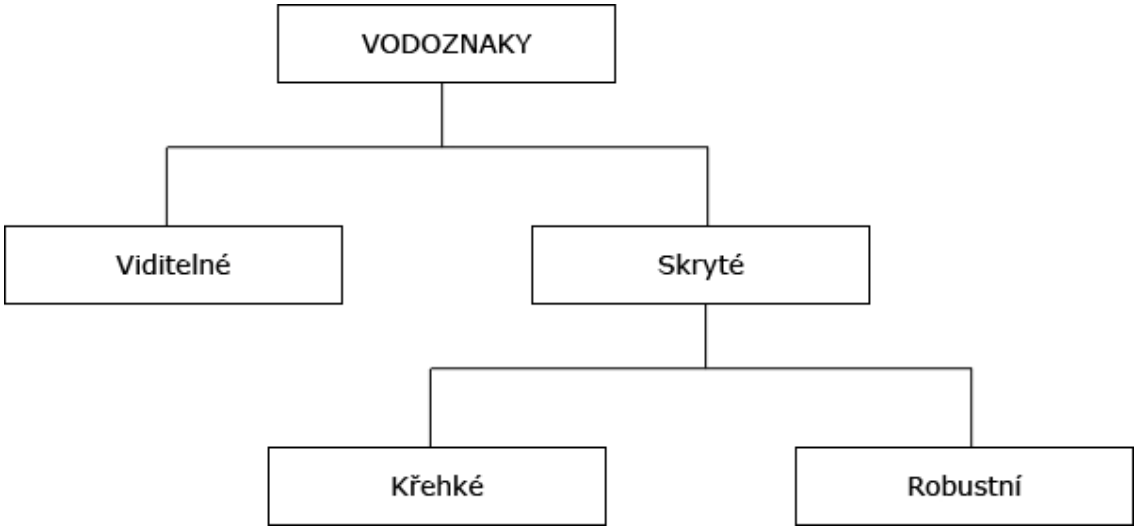
Vodoznačení: Účelem vodoznační je ochrana autorských práv. Jedná se o vložení přídavné informace do nezabezpečených multimediálních dat tak, aby modifikace těchto informací byla smyslově nepostřehnutelná a zároveň odolná proti případným útokům.

Vytažení vodoznaku: Jedná se o proces výběru vodoznaku z chráněných dat tak, aby ho bylo možné porovnat s vloženým vodoznakem.

Detekce vodoznaku: Je rozhodovací proces, jehož výsledek nám může říct, zda data byla nebo nebyla označená vodoznakem.

Útoky: Hlavním cílem útoků je znehodnocení či úplné odstranění vloženého vodoznaku. To má za následek neumožnění shody vloženého a vytaženého vodoznaku a tudíž nepotvrzení vlastnického práva.

1.2. Klasifikace digitálních vodoznaků



Obr. 1.1: Znázornění klasifikace vodoznaků.

V technice digitálních vodoznaků se používají různé typy vodoznaků, které v zásadě můžeme rozdělit do těchto skupin (viz. obr. 1.1) [1],[9].

Viditelné vodoznaky jsou loga, vizuální obrazce či jiné značky, které částečně nebo zcela překrývají určitou oblast statického obrazu, resp. videa. Těmito vodoznaky si můžeme představit obdobu peněžních (papírových) vodoznaků. Používají se pro ochranu videa, statických obrazů či textu.

Skryté vodoznaky nejsou běžně viditelné, jsou vloženy do nezabezpečených dat, aby pokud možno nebyl narušen původní informační obsah. Používají se pro ochranu obrazových, zvukových, video i textových dat. Skryté vodoznaky můžeme dále rozdělit na křehké a robustní.

Křehké vodoznaky se vyznačují svou jednoduchostí a sníženou odolností proti různým útokům na vodoznačný datový obsah. Jakmile je vodoznačný datový obsah modifikován, stávají se vložené vodoznaky nedetekovatelné. Skupina těchto vodoznaků se používá k detekci různých modifikací původních vodoznačných dat.

Robustní vodoznaky jsou navrženy tak, aby odolávaly manipulaci s daty a chrání do značné míry před útoky, snažící se o prolomení zabezpečených dat. Používají se hlavně pro ochranu vlastnického práva autora.

1.3. Požadavky na digitální vodoznaky

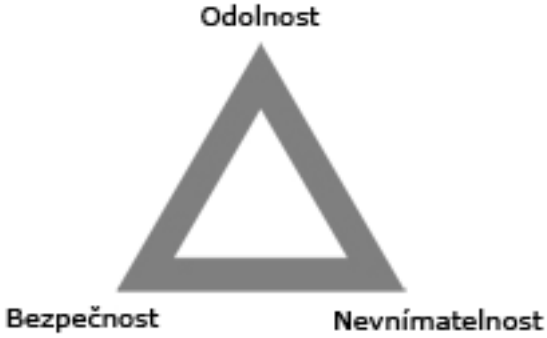
K efektivnímu využití vodoznační nechráněných dat je potřeba splnit několik požadavků [3], [4], [7]. Mezi základní požadavky u digitálních vodoznaků patří zejména odolnost, nevnímatelnost a bezpečnost.

Odolnost: Nemělo by být možné bez znalosti použité metody a tajného klíče odstranit vodoznak nebo jej znehodnotit tak, že se stane nečitelným. Modifikace zdrojových dat mohou být úmyslné (útoky) nebo neúmyslné (komprese, oříznutí, rotace atd.).

Nevnímatelnost: Změny způsobené vložením vodoznaku by neměly přesáhnout práh citlivosti zraku člověka. Je tedy důležité dobře zvolit práh, pod kterým vzorky vodoznaku nezpůsobí vnímatelné optické nebo zvukové změny. Vodoznak je tedy považován za nevnímatelný nebo skrytý, pokud je nepostřehnutelný lidskými smysly. Toto rozhodování a volba prahu je založená na vlastnostech lidského zraku (HVS).

Bezpečnost: Bezpečnost většiny dnešních systémů s vodoznaky je založena na používání jednoho nebo několika kryptografických klíčů, což ztěžuje přístup a následné odstranění vodoznaku. Jakmile ale útočník odhalí princip vodoznační a zná přesná místa, kde jsou skryta data vodoznaku, může snadno provést jeho odstranění.

Tyto tři nejzákladnější požadavky jsou zobrazeny jako vrcholy trojúhelníku (obr. 1.2) [4]. Trojúhelník nám naznačuje, je-li na jeden požadavek kladen velký důraz, zbylé dva požadavky jsou oslabené. Například požadavek na vysokou odolnost vodoznaku způsobí vnímatelné (viditelné) změny v zabezpečených datech a naopak.



Obr. 1.2: Zobrazení základních požadavků na vodoznak

Mezi rozšiřující požadavky na vodoznak lze zařadit např. složitost, spolehlivost detekce a kapacitu.

Složitost: Pro vyhodnocení složitosti se používá množství času spojené s odstraněním vodoznaku. Obecně je doporučeno navrhovat algoritmy vkládání vodoznaku tak náročné, aby jejich prolomení trvalo útočníkovi takovou dobu, po které by se odstranění vodoznaku stalo již bezvýznamné.

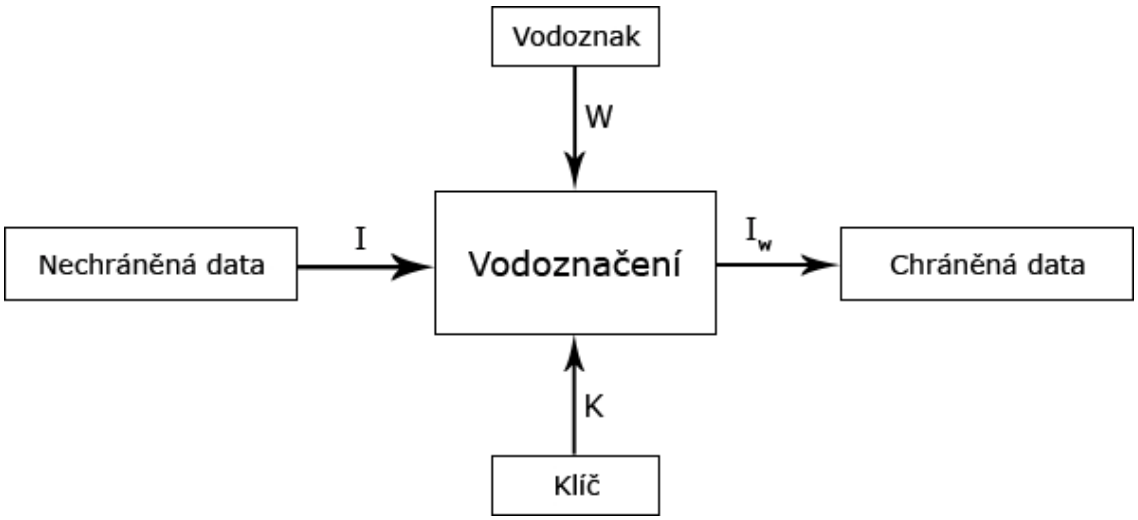
Spolehlivost detekce: Vodoznak by měl představovat dostatečný a spolehlivý důkaz o vlastnických právech k testovaným datům.

Kapacita: Kapacita udává množství nadbytečné (vodoznačné) informace, která může být uložena do zdrojových dat. Kapacita vodoznaku je velmi důležitá vlastnost a úzce souvisí s odolností. Pokud totiž zdrojová data obsahují velké množství vložených informací, stává se vodoznak v případě útoku snáze detekovatelným. Naproti tomu při vložení minimálního počtu informačních bitů, které jsou obsaženy jen ve velmi malé oblasti zdrojových dat, je vodoznak prakticky odstraněn jakoukoli modifikací. Je tedy vždy důležité dobře rozhodnout jaké množství vložené informace je vhodné pro konkrétní případ.

1.4. Obecný princip zabezpečení digitálními vodoznaky

Tato část kapitoly je věnována principu vložení vodoznaku a jeho vytažení/detekce z chráněných dat. Dosud známé vodoznačící systémy používají obecně stejné funkční bloky [3], [4] a lze je popsat podle následujících obrázků (1.3, 1.4).

1.4.1. Základní princip systému vložení vodoznaku



Obr. 1.3: Obecné blokové schéma vodoznačení

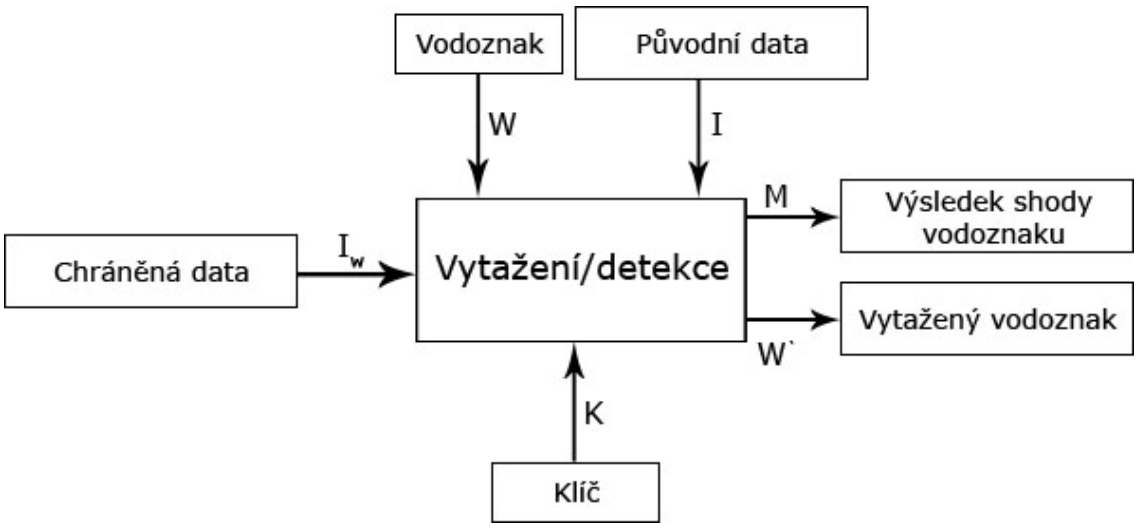
K zabezpečení datového obsahu se používá třech vstupních parametrů. Původní originální nechráněná data, vodoznak a šifrovací klíč (viz. obr. 1.3). Šifrovací klíč může, ale nemusí být součástí sytému vodoznačení. Jeho použití však zvyšuje bezpečnost vloženého vodoznaku, a tím se zároveň zvyšuje ochrana originálních dat před neoprávněnými uživateli. Některé vodoznačící systémy používají buď jeden nebo i kombinaci více šifrovacích klíčů. Výstupem sytému vodoznačení jsou chráněná data obsahující vodoznak.

Vodoznačení lze vyjádřit pomocí funkce (E_K) [7]:

$$E_K(I, W, K) = I_W, \tag{1.1}$$

kde I jsou originální data, W je vodoznak, K šifrovací klíč a I_W jsou výstupní vodoznačná data.

1.4.2. Základní princip systému vytažení/detekce vodoznaku



Obr. 1.4: Obecné blokové schéma vytažení/detekce vodoznaku

K vytažení/detekci vodoznaku je použito čtyř vstupních parametrů. Chráněná data, vodoznak, původní datový obsah a šifrovací klíč. Proces vytažení vodoznaku (viz. obr. 1.4) je opačná operace k procesu vložení. Výstupem tohoto systému je vytažený vodoznak *W`* a shoda *M* vytaženého vodoznaku s vloženým.

Funkci vytažení vodoznaku (D_K) lze vyjádřit [7]:

$$D_K (I_W, W, K) = W`. \tag{1.2}$$

Podle počtu vstupů a výstupů při vytažení/detekci vodoznaku existují 3 skupiny zabezpečovacích systémů [2], [3], které jsou uvedeny v následující kapitole.

1.5. Zabezpečovací systémy s digitálními vodoznaky

Privátní systémy

Tento systém je charakteristický tím, že k vložení vodoznaku do originálních dat používá soukromý klíč. Při vytažení/detekci vodoznaku vyžaduje kromě soukromého klíče i originální data. Tento systém se dále dělí na dva typy:

Typ I Je schopen vytáhnout vodoznak i ze zkreslených dat, ale vyžaduje původní originální data.

Typ II Vyžaduje kromě původních originálních dat i kopii vloženého vodoznaku. Výstupem z bloku míry shody vodoznaku (viz. obr. 1.4) je potvrzení/nepotvrzení vlastnického práva autora (1, 0 – Ano, Ne).

Privátní systém zabezpečení vodoznakem dokáže vrátit změny v informačních datech způsobené útočníkem, protože používá na vstupu originální data.

Poloprivátní systémy

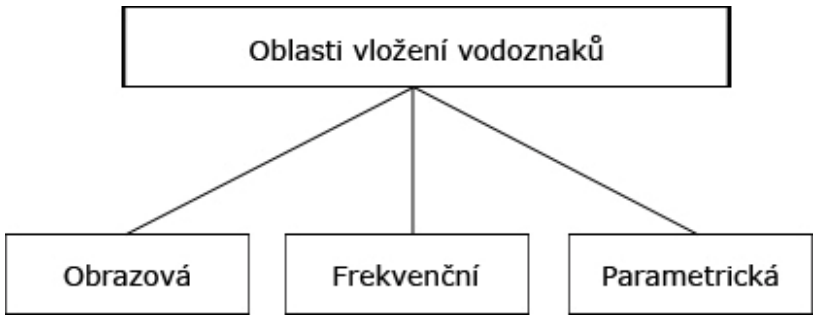
Jsou odvozeny z privátních systémů typu II, ale nepoužívají na vstupu původní originální data. Při vytažení/detekci vyžadují soukromý klíč a kopii vloženého vodoznaku.

Veřejné systémy

Tyto systémy nepotřebují k vytažení vodoznaku z chráněných dat původní originální data, ani kopii vloženého vodoznaku. K vytažení je potřeba znát soukromý klíč. K procesu vodoznačení používají veřejný klíč.

1.6. Oblasti vkládání vodoznaků

Metody pro vložení vodoznaků je možné v současné době rozdělit do tři skupin [4] podle principů vkládání vodoznaku do zdrojových obrazových dat (obr. 1.5).



Obr. 1.5: Možné oblasti vložení vodoznaků

Obrazová oblast

Metody využívající obrazové části vkládání vodoznaků jsou založené na modifikaci jednotlivých obrazových bodů (pixelů). Využívá se přitom nedokonalosti lidského vnímání, kde lidské oko je schopné rozeznat maximálně 90 úrovní jasové složky [4]. Mezi nejčastější metodu realizující modifikaci obrazových prvků patří metoda, která modifikuje nejméně významné bity, zvaná LSB. Metoda LSB je založená na jednoduché myšlence nahradit nejméně významný bit v obraze jedním bitem vodoznaku.

V dnešní době je tato metoda zřídka používaná z důvodu malé odolnosti takto vloženého vodoznaku. Výhoda spočívá v její jednoduchosti.

Frekvenční oblast

Metody pracující ve frekvenční oblasti obrazu jsou založené na modifikaci jednotlivých transformačních koeficientů. Při vkládání vodoznaku se nejprve provede transformace zdrojových dat do prostoru transformačních koeficientů. Výběrem transformačních koeficientů určených k modifikaci se mezi sebou liší jednotlivé vodoznačící metody. Mezi nejčastěji používané transformace jsou diskrétní kosinová transformace (DCT) a diskrétní vlnková transformace (DWT). Inverzní transformací modifikovaných koeficientů se získají původní obrazová data, ve kterých je vložený vodoznak.

Metody v transformační oblasti jsou v dnešní době nejvyužívanějšími metodami vodoznačení v obraze. U těchto metod je možné nastavit různou odolnost vodoznaku.

Parametrická oblast

Techniky vložení vodoznaku v parametrické oblasti využívají transformaci obrazu do parametrického prostoru. Jsou založené na modifikaci některých parametrů v originálním obraze. Příkladem této techniky je metoda vkládání vodoznaku, založená na fraktálovém kódování obrazu, kde bývají upravovány parametry jasu nebo kontrastu. Další metodou vodoznačení v parametrické oblasti je metoda založená na změně barevné matice RGB, kde je upravován například parametr sytosti barvy [4].

Výsledné vodoznaky, vložené metodou využívající fraktálové kódování, jsou odolné zejména proti kompresi nebo filtrování signálu.

1.7. Hodnocení kvality obrazu po vložení vodoznaku

V praxi lze hodnotit kvalitu obrazu dvojím způsobem. Subjektivně (využitím pozorovatelů) nebo objektivně (využitím měření).

Subjektivní hodnocení

Jedná se o vizuální hodnocení kvality obrazu člověkem. Při hodnocení je obvykle k dispozici celá řada obrazů dostupná k posouzení. Tyto obrazy jsou generovány s jedním pevným parametrem a měnícím se druhým parametrem (nebo množinou parametrů). Tato metoda hodnocení je nákladná a posuzování trvá dlouhou dobu, protože lidské oči jsou lehce unavitelné.

Objektivní hodnocení

Uvažujme originální vstupní obraz jako funkci dvou proměnných *f(x,y)*, kde *x a y* jsou souřadnice bodů v obraze. Nyní definujeme výstupní (vodoznačenou) funkci *g(x,y)* a určíme chybovou funkci *e(x,y)* podle [8]:

$$e(x,y) = f(x,y) - g(x,y). \tag{1.3}$$

Střední kvadratická chyba *MSE* (*mean square error*) je:

$$MSE = \frac{1}{MN} \sum_{x=0,y=0}^{M-1,N-1} e(x,y)^2 , \tag{1.4}$$

kde *M* a *N* představují horizontální a vertikální rozměry obrazu.

Střední absolutní chyba *MAE* (*mean absolute error*) je:

$$MAE = \frac{1}{MN} \sum_{x=0,y=0}^{M-1,N-1} \left| e(x,y) \right| . \tag{1.5}$$

Pokud známe *MSE*, můžeme dále definovat odstup signálu od šumu (signal-noise ratio, *SNR*):

$$SNR = 10 log_{10} \left(\frac{\sum_{x=0,y=0}^{M-1,N-1} g(x,y)^2}{MN \cdot MSE} \right) . \quad \text{(dB)} \tag{1.6}$$

V praxi se ale častěji používá špičková hodnota odstup signál-šum (*peak signal-to-noise ratio*, *PSNR*):

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right). \qquad \text{(dB)} \tag{1.7}$$

Čím větší *PSNR*, tím je lepší kvalita vodoznačného obrazu ke vztahu k původnímu obrazu.

Pro posouzení shody mezi originálním a vytaženým vodoznakem používáme normalizovanou vzájemnou korelaci (*normalized cross-correlation*, *NCC*) [6]:

$$NCC = \left(\frac{\sum_{i=0,j=0}^{I-1,J-1} W_{ij} W'_{ij}}{\sum_{i=0,j=0}^{I-1,J-1} (W_{ij})^2}\right), \tag{1.8}$$

kde I a J představují horizontální a vertikální rozměry vodoznaků. W je originální vodoznak, W' vytažený vodoznak. Výstup funkce je v rozmezí hodnot 0 až 1.

Objektivní způsob hodnocení kvality je možné brát jako správný, ale jeho vypovídací hodnota není zcela směrodatná. Například v objektivním měření se neprojeví jinak rušivý artefakt vodoznaku. Dále si je také třeba uvědomit, že obrazový vjem v lidském mozku závisí na podnětu nelineárně.

Na druhou stranu je pořízení takového výsledku málo nákladné a snadno opakovatelné. V nejlepším případě jsou k hodnocení kvality obrazu použity jak subjektivní, tak objektivní metody měření.

1.8. Útoky na vodoznaky

Cílem útoků na chráněnou obrazovou informaci je dosáhnout znehodnocení anebo úplné odstranění vloženého vodoznaku. Tyto útoky v dnešní době můžeme stále rozdělit do čtyř skupin [2] (obr. 1.6).

Obr. 1.6: Třídy útoků na vodoznaky

Útoky odstraňující vodoznak

Mají za cíl úplně odstranit z chráněných dat vložený vodoznak bez znalostí algoritmu vodoznační a případných použitých klíčů. Tato kategorie útoků zahrnuje typy útoků, jakými jsou např. filtrace obrazu, kvantizace, ztrátová komprese, přidání šumu do obrazu atd. Většinou ne všechny z nich úplně odstraní vodoznak, ale značně ho poškodí.

Geometrické útoky

Geometrické útoky na rozdíl od předchozích úplně neodstraňují vložený vodoznak, ale způsobují jeho zkreslení při vytažení. Geometrické útoky využívají různé operace s chráněnými obrazovými daty jako je např. ořezání, rotace, deformace, projektivní transformace, posun, zkosení, změna měřítka obrazu.

Kryptografické útoky

Cílem je prolomit kryptografickou bezpečnost techniky vodoznaků a tak najít cestu na odstranění vodoznaku, či vložení falešného vodoznaku. Jedním z typů kryptografických útoků je metoda hrubého násilí (*brute force*). Nevýhodou kryptografických útoků je velká výpočetní náročnost, a proto se používají velice zřídka.

Protokolové útoky

Napadají celkovou koncepci techniky vodoznaků a jejich aplikaci. Jeden typ protokolových útoků je založený na koncepci invertibilních vodoznaků. Princip spočívá v tom, že útočník využije přítomnost vodoznaku v chráněných datech. Inverzní funkcí vodoznak vloží do vlastních obrazových dat a odčítá svůj vlastní vodoznak z takto označených obrazových dat [2]. To může vyvolat nejasnosti s vlastnickým právem chráněné informace. Řešením tohoto problému je, že autor použije jednosměrnou funkci na vložení vodoznaku.

Jinačím typem protokolových útoků je útok kopírováním (*copy attack*). Cílem útoku kopírováním není znehodnocení nebo úplné odstranění vodoznaku, ale odhadnutí vodoznaku v chráněných datech a následné překopírování do cílových dat. Proces kopírování vodoznaku vyžaduje znalost algoritmu vodoznačení a popřípadě použitého tajného klíče, který byl součástí vložení vodoznaku.

2. Systémy určené k hodnocení vodoznačení

Tato druhá část kapitoly je věnována aplikačním nástrojům sloužícím k hodnocení vodoznačení tzv. „*benchmarky*“. Hlavním účelem těchto nástrojů je charakterizovat a upozornit na výhody a slabé stránky vodoznačících metod. Výsledky testů umožňují jejich efektivní porovnávání. Každý z těchto nástrojů obsahuje v sobě funkční bloky simulující útoky na zabezpečená obrazová data.

V dnešní době máme k hodnocení parametrů digitálních vodoznaků nejméně tři veřejné aplikační nástroje Stirmark, Optimark a Checkmark [1]. Vzhledem k vhodnosti použití v této práci a po konzultacích s vedoucím diplomové práce, jsme se rozhodli k použití nástroje Checkmark. Proto se v následujícím textu budu zaměřovat spíše na něj.

2.1. Stirmark

Stirmark je jeden z prvních veřejných nástrojů k hodnocení odolnosti vodoznačených dat. První verze byla publikována v roce 1997 (Penticolas, Anderson, Kun). Jeho poslední verze 4.0 v roce 2003. Tento nástroj je dostupný z oficiálních stránek na adrese <*http://www.petitcolas.net/fabien/watermarking/stirmark/*>.

2.2. Optimark

Optimark je další z nástrojů sloužící k hodnocení vodoznační. Byl uveden v roce 2002. Vyznačuje se graficko-uživatelským rozhraním. Tento nástroj odstraňuje některé nedostatky ze Stirmarku a umožňuje hodnotit i video a audio chráněný obsah. Je dostupný z oficiálních stránek na adrese <*http://poseidon.csd.auth.gr/optimark/*>.

2.3. Checkmark

Checkmark byl vyvinutý na univerzitě v Ženevě v roce 2001 (Pereira). Je vytvořen v programovacím prostředí MATLAB a běží pod Windows a Unix. Poskytuje efektivní a účinný nástroj k hodnocení technologií vodoznačení. Jeho poslední verze 1.2 je volně ke stažení na stránkách *<http://watermarking.unige.ch/Checkmark/>*. Checkmark v sobě zahrnuje nové vylepšené třídy útoku oproti předchozím nástrojům, jimž například jsou vlnková komprese, projektivní transformace, deformace v obraze, podvzorkování a nadvzorkování. Na základě otevřené platformy si lze vytvořit i své vlastní formy útoků. Byly také implementovány nové metody pro hodnocení kvality vodoznačného obrazu, vážená špičková hodnota signál-šum (*weighted PSNR*) a Watsonová metrika (*Watson metric*). Výsledky testů z nástroje Checkmark jsou přehledně generovány do tabulek v HTML formátu.

2.3.1. Konfigurace nástroje Checkmark

Aby bylo možné pracovat s tímto nástrojem, je potřeba ho správně nastavit. Jedná se o první praktickou část práce. Aplikace byla odladěna v prostředí MATLAB ve verzi 7.1 (R14, SP3)

Nastavení souboru *getconfig.m*:

V tomto souboru nastavujeme hlavně cesty k samotnému programu, jednotlivým obrazům a výstupům.

checkmarkPath = zadat cestu k nástroji Checkmark.

SETUP.imagepath = zadat cestu k vodoznačeným obrazům. Musí zde být uložený vodoznačený obraz, tak i jeho originál.

SETUP.attackedsubdir = cesta pro ukládání vodoznačených obrazů po útocích.

SETUP.applicname = pro jaké aplikační účely se má Checkmark používat, postačí zadat v našem případě *'copyright'*.

SETUP.numims = zadat počet vodoznačených obrázků na vstupu.

SETUP.techname = zadat název metody vodoznačení.

SETUP.mainHTMLpage = zadat název výstupní HTML stránky.

SETUP.HTMLPATH = cesta k HTML stránce.

SETUP.HTML_BASEHREF = nastavíme stejně cestu jako v předchozím případě.

SETUP.HTML_IMAGES_PATH = cesta k obrázkům sloužící jako pozadí vygenerovaných výsledků.

SETUP.JARSPATH = nadefinování cesty k JAR souborům (*xalan.jar*, *xerxes.jar*), slouží k vygenerování HTML stránky z XML formátu.

Nastavení souboru *testDetector.m*:

Výstupem skriptu je vygenerování XML formátu, kde jsou jednotlivé výsledky testu. Na řádku 25 a 82 je potřeba změnit příkaz: „*com1=sprintf('cd %s',dir1); eval(com1);*“ na „*com1=cd(dir1);*“.

Příkaz „*detectionresult = executedetector(fname);*“ volá funkci *executedetector.m*, která musí být upravena podle metody vytažení vodoznaku s rozhodovací funkcí (0,1), zda je vytažený vodoznak rozpoznatelný s originálem.

Nyní máme vše potřebné nastavené a celý proces testování s vygenerováním výsledků spustíme pomocí souboru *doall.m*.

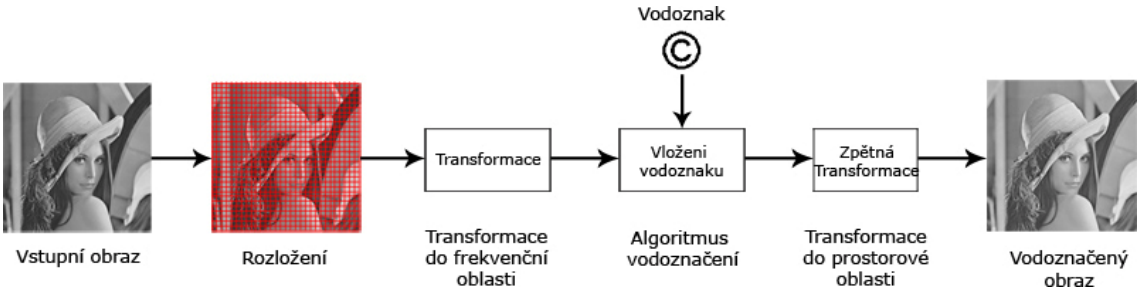
3. Realizace metod vodoznačení

K realizaci metod vodoznační byla vybrána po konzultacích s vedoucím diplomové práce transformační oblast. Metody vkládání vodoznaku v transformační oblasti jsou v dnešní době nejrozšířenějšími a výhodou je nastavení různé odolnosti vodoznaku podle potřeby. Základem vytvořených metod je diskrétní kosinová transformace (DCT). Funkční aplikace jsou vytvořeny a odzkoušeny podle zadání v prostředí MATLAB.

3.1. Realizace první metody

Metoda popsaná v [9] je založená na záměně frekvenčních koeficientů v pásmu středních frekvencí v transformovaném bloku (viz. obr. 3.2). Podle níže popsaného algoritmu se porovnávají mezi sebou dva DCT koeficienty sloužící k zakódování jednoho bitu tajné zprávy (vodoznaku). Při procesu vytažení vodoznaku je potřeba pouze kopie vloženého vodoznaku.

3.1.1. Vložení vodoznaku do obrazu



Obr. 3.1: Postup realizace metody vodoznační ve frekvenční oblasti

Celý proces vložení vodoznaku je znázorněn na obrázku 3.1. Jako vstupní obraz v odstínech šedi byla k účelu zabezpečení použita Lenna (512×512 pix, 8 bit). Následuje rozdělení obrazu do bloků. Velikost bloku jsem použil stejnou jako u standardu JPEG a to 8×8 pixelů. Každý z těchto bloků je posléze samostatně převeden do frekvenční oblasti pomocí diskrétní kosinové transformace. Výpočet frekvenčních koeficientů obrazu o velikosti $N \times N$ se provádí pomocí dvourozměrné diskrétní kosinové transformace (2D-DCT) podle vztahu [5]:

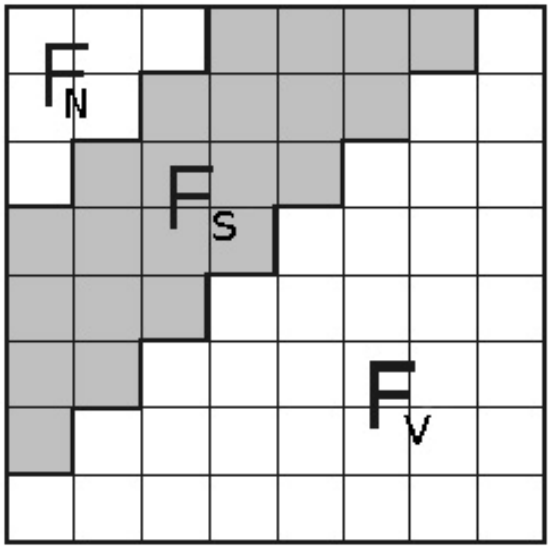
$$\mathbf{Y} = \mathbf{AXA}^{\mathrm{T}}, \tag{3.1}$$

kde **Y** je výstupní matice koeficientů, **X** je vstupní matice vzorků, **A** je transformační matice. Prvky transformační matice lze vyjádřit vztahy [5]:

$$A_{ij} = C_i \cos\frac{(2j+1)i\pi}{2N},\ C_i = \sqrt{\frac{1}{N}}\ (\text{pro } i=0),\ C_i = \sqrt{\frac{2}{N}}\ (\text{pro } i>0) \tag{3.2}$$

Vysokofrekvenční složky reprezentují malou část energie obrazu a představují pouze informace o detailech obrazu. Většina energie je soustředěna v nízkofrekvenční oblasti.

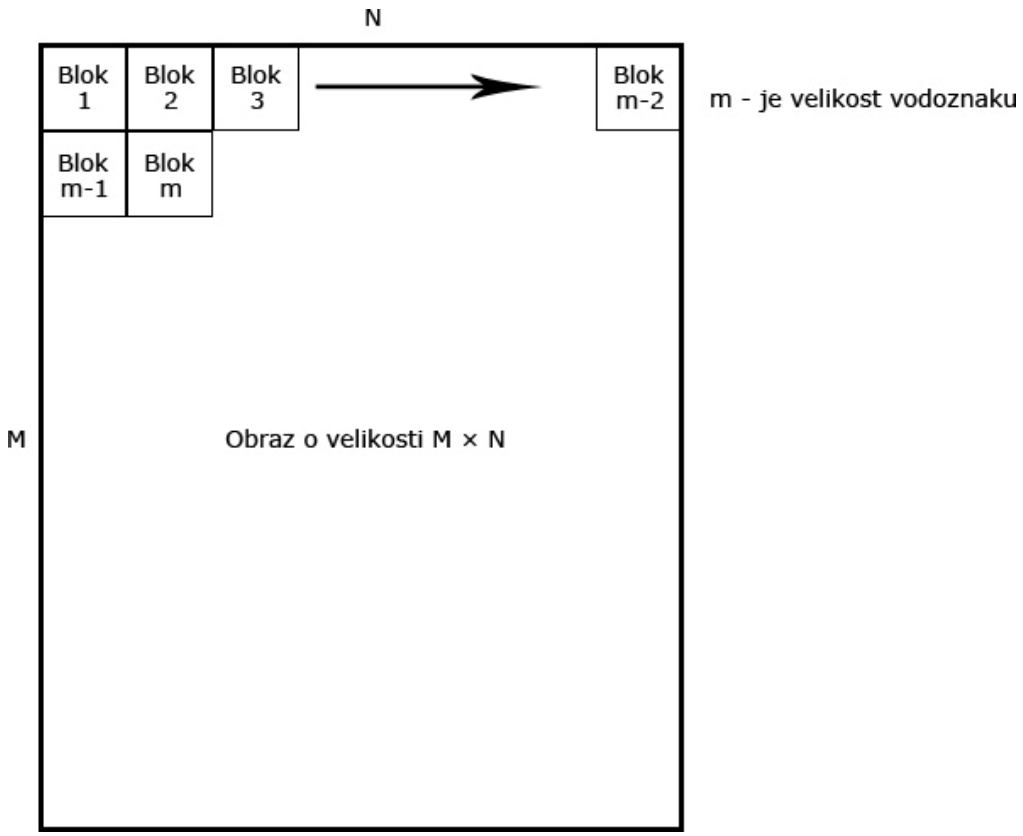
Je důležité určit hlavní požadavky na vodoznak. Pokud by byl vodoznak vložen do nízkofrekvenční oblasti F_N, dosáhlo by se vysoké odolnosti proti různým modifikacím, ale současně by se mohl porušit jeden z požadavků kladený na vodoznak - nevnímatelnost. Pokud je ale požadována vysoká nevnímatelnost, vodoznak se vkládá do vysokofrekvenční oblasti F_V, tím se ale stává velice málo odolným. Proto vhodnou volbou se jeví kompromis zmíněných podmínek [9]. Vhodnou oblastí pro vložení vodoznaku je oblast středních frekvencí F_S (obr. 3.2).



Obr. 3.2: Rozložení spektra v transformovaném bloku

Do každého bloku je pak vložen jeden bit vodoznaku. Výběr bloků, do kterých budeme vkládat vodoznak, může být napevno dán (použito u této realizace) nebo použit

pseudonáhodný výběr podle šifrovacího klíče. Vybírání bloků je realizováno v horní části obrazu směrem zleva doprava až do velikosti vodoznaku (viz. obr. 3.3).



Obr. 3.3: Znázornění výběru bloků určených k vložení vodoznaku

Nyní si musíme stanovit, které koeficienty z oblasti středních kmitočtů budou použity pro vložení vodoznaku. Metoda uvedená v [9] při vkládání vodoznaku používá obecně koeficienty $B_i(u1, v1)$, $B_j(u2, v2)$. Při vkládání vodoznaku musí být použity takové koeficienty, které jsou při kompresi JPEG kvantovány stejnými hodnotami [9] z důvodu zachování podmínek nerovnosti u vodoznačení, které jsou popsány dále v textu. Za vhodné pozice koeficientů z pomyslné oblasti středních kmitočtů jsem zvolil $B_1(5,2)$ a $B_2(4,3)$ orámované v tab. 1 červenou barvou.

Tab.1: Kvantizační matice u JPEG komprese

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Metoda vložení vodoznaku je založena na záměně vybraných koeficientů. Vstupní hodnota vodoznaku může být černá nebo bílá (0, 1) viz. obrázek 3.1. Pokud aktuální hodnota vodoznaku je „1“ a neplatí následující podmínka $Bi(ui, vi) > Bj(uj, vj)$, je potřeba přehodit mezi sebou koeficienty. Pokud je aktuální hodnota vodoznaku „0“ a neplatí následující podmínka $Bi(ui, vi) < Bj(uj, vj)$, je potřeba mezi sebou prohodit koeficienty pro splnění podmínky. Tudíž můžeme napsat:

Vstupní hodnota vodoznaku $W = 0$, $Bi(ui, vi) < Bj(uj, vj) \rightarrow$ v pořádku,
$Bi(ui, vi) > Bj(uj, vj) \rightarrow$ záměna koeficientů.

Vstupní hodnota vodoznaku $W = 1$, $Bi(ui, vi) > Bj(uj, vj) \rightarrow$ v pořádku,
$Bi(ui, vi) < Bj(uj, vj) \rightarrow$ záměna koeficientů.

Tímto jsme jednoznačně zakódovali vstupní hodnoty vodoznaku do frekvenční oblasti obrazu.

Robustnost vodoznační může být vylepšena zahrnutím tzv.“síly“ vodoznaku k podle nerovnosti:

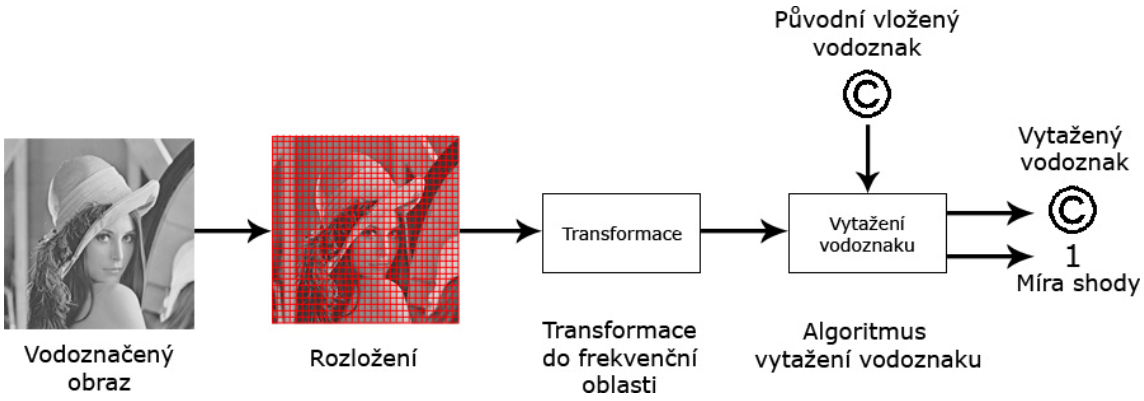
$$Bi(ui, vi) - Bj(uj, vj) > k \tag{3.3}$$

Pokud je hodnota k menší nebo rovna hodnotě rozdílu koeficientů, pak se nic neděje. Pokud je však hodnota k větší, provede se úprava hodnot DCT koeficientů tak, aby výsledná hodnota rozdílu byla rovna nastavené hodnotě. Úprava koeficientů však nesmí změnit podmínky nerovnosti vodoznační, tedy pokud byl první koeficient po vložení vodoznaku větší než druhý, musí to tak zůstat i po dodatečném nastavení robustnosti vodoznaku. Je potřeba mít stále na paměti, že čím větší hodnota robustnosti, tím jsou více viditelné artefakty vodoznaku v obraze.

Abychom získali výsledný vodoznačný obraz je potřeba převod z frekvenční oblasti zpět do prostorové, pomocí zpětné diskrétní kosinové transformace (IDCT) [5]:

$$\mathbf{X} = \mathbf{A}^{T}\mathbf{Y}\mathbf{A} \tag{3.4}$$

3.1.2. Vytažení vodoznaku z obrazu



Obr. 3.4: Postup realizace vytažení vodoznaku z frekvenční oblasti

Proces vytažení vodoznaku je opačná operace k procesu vložení (obr. 3.4). K vytažení vodoznaku je potřeba dvou vstupních parametrů, což jsou vodoznačný obraz a původní vodoznak. Výstupem je vytažený vodoznak a míra shody vytaženého vodoznaku s vloženým.

Kroky postupu po algoritmus vytažení vodoznaku jsou stejné jako u vložení, a proto nebudou znova popisovány. Vytažení vodoznaku spočívá v porovnávání frekvenčních koeficientů v jednotlivých vodoznačených blocích, v našem případě koeficienty $B_1(5,2)$ a $B_2(4,3)$. Pokud je první koeficient větší než druhý, zapíše se do výstupního pole vytaženého vodoznaku hodnota „1“-bílá. Jestliže tomu tak není, zapíše se „0“-černá. Můžeme napsat:

$$Bi(ui, vi) > Bj(uj, vj) \rightarrow \text{výstup „1“}$$
$$Bi(ui, vi) < Bj(uj, vj) \rightarrow \text{výstup „0“}$$

Po porovnávání jednotlivých vodoznačených bloků máme úplnou informaci o vytaženém vodoznaku. K určení míry shody mezi vytaženým a originálním vodoznakem byla použita normalizovaná vzájemná korelace (viz. rov. 1.8). Na blokovém obrázku 3.4 je míra shody rovna „1“ tzn. vytažený vodoznak je zcela stejný

jako jeho originál. To ovšem platí v ideálním případě. V poslední části této kapitoly jsou provedeny testy odolnosti realizované metody.

3.1.3. Test odolnosti metody

Záměrné útoky na chráněná obrazová data způsobí znehodnocení vodoznaku až jeho úplné odstranění. Kapitola se zabývá vyhodnocením odolnosti realizované metody. K simulaci útoků na chráněné obrazové informace byl použit aplikační nástroj Checkmark popsaný v kapitole 2.

K účelu zabezpečení byl použit obraz Lenny (obr. 3.5a) s rozměry 512×512 pixelů v odstínech šedi. Vodoznak (obr. 3.5c) o rozměrech 60×60 pixelů v černobílém provedení. Výstup vodoznační je vidět na obrázku 3.5b. Odolnost byla nastavena s ohledem na nevnímatelnost a robustnost vodoznaku na hodnotu $k = 8$.

a) b)

c)

Obr. 3.5. Lenna: a) nechráněný obraz, b) vodoznačený obraz s *PSNR* = 44,21 dB, c) vložený vodoznak

K stanovení hranice, zda je vytažený vodoznak rozeznatelný se svým originálem, jsem uvážil podle svého vizuálního subjektivního dojmu (obr. 3.6). Hranice je nastavena na hodnotu *NCC* = 0,79. Vytažený vodoznak je považován za shodný se svým originálem, pokud hodnota *NCC* je větší nebo rovna hodnotě 0,79. V opačném případě je vytažený vodoznak považován se svým originálem za neshodný.

Obr. 3.6: Vytažený vodoznak s hodnotou *NCC*=0,798

Útok kompresí JPEG:

Tab. 2: Hodnoty testu odolnosti po kompresi JPEG

Stupeň kvality JPEG *Q* [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
100	1	1
90	1	1
85	1	1
80	0,999	1
75	0,925	1
60	0,683	0
50	0,643	0
40	0,633	0
30	0,632	0
25	0,668	0
15	0,699	0
10	0,74	0

Obr. 3.7. Útok kompresí JPEG: a) Q=75, b) Q=10, c) vytažený vodoznak pro Q=75, d) vytažený vodoznak pro Q=10

Z tabulky 2 je patrné, že vložený vodoznak je odolný proti kompresi JPEG do parametru Q=75. S vyšším stupněm komprese se stává vložený vodoznak nedetekovatelný (obr. 3.7d).

Útok vlnkovou kompresí:

Tab. 3: Hodnoty testu odolnosti po vlnkové kompresi

Kompresní poměr [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
1:1	1	1
1:2	1	1
1:5	0,987	1
1:10	0,798	1
1:13	0,681	0
1:16	0,652	0
1:20	0,606	0
1:26	0,572	0
1:40	0,548	0
1:80	0,55	0

a) b)

c) d)

Obr. 3.8. Útok vlnkovou kompresí: a)komprese1:5, b)komprese1:40, c) vytažený vodoznak z komprese 1:5, d) Vytažený vodoznak z komprese 1:40

Do kompresního poměru 1:10 vlnkové transformace vložený vodoznak byl téměř shodný s jeho originálem (viz.tab. 3).

Útoky založené na filtrování obsahu:

Tab. 4: Hodnoty testu odolnosti po filtraci obsahu

Filtr	Velikost filtrovacího okna [pixel]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
Gaussovské rozostření	3×3	1	1
Gaussovské rozostření	5×5	1	1
Zostření	3×3	0,998	1

a) b)

c) d)

Obr. 3.9. Útok filtrováním obsahu: a)rozostření - filt. okno 5×5 pix., b)zostřením, c)vytažený vodoznak z rozostření-filt.okno 5×5 pix., d)vytažený vodoznak ze zostření

Útoky, založené na filtraci obsahu v tomto testu, neměly žádný vliv na znehodnocení vloženého vodoznaku, jak je patrné z tab. 4 a obrázků 3.9.

Útoky založené na převzorkování obrazového signálu:

Tab. 5: Hodnoty testu odolnosti po převzorkování obrazového signálu

Typ [-]	Míra podvzorkování [-]	Míra nadvzorkování [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
1	0,75	1,33	0,961	1
2	0,5	2	0,816	1
3	0,75	1,3	0,506	0
4	0,5	1,9	0,49	0

a) b)

Obr. 3.10 Útok převzorkováním: a) vodoznačný obraz po převzorkování typu 1, b) jeho vytažený vodoznak *NCC*=0,961

Převzorkování typu 1 a 2 nezmodifikovalo vložený vodoznak do takové míry, aby se stal po algoritmu detekce nečitelným (tab. 5, obr. 3.10b). Detekce vodoznaku byla u převzorkování typu 3 a 4 neúspěšná.

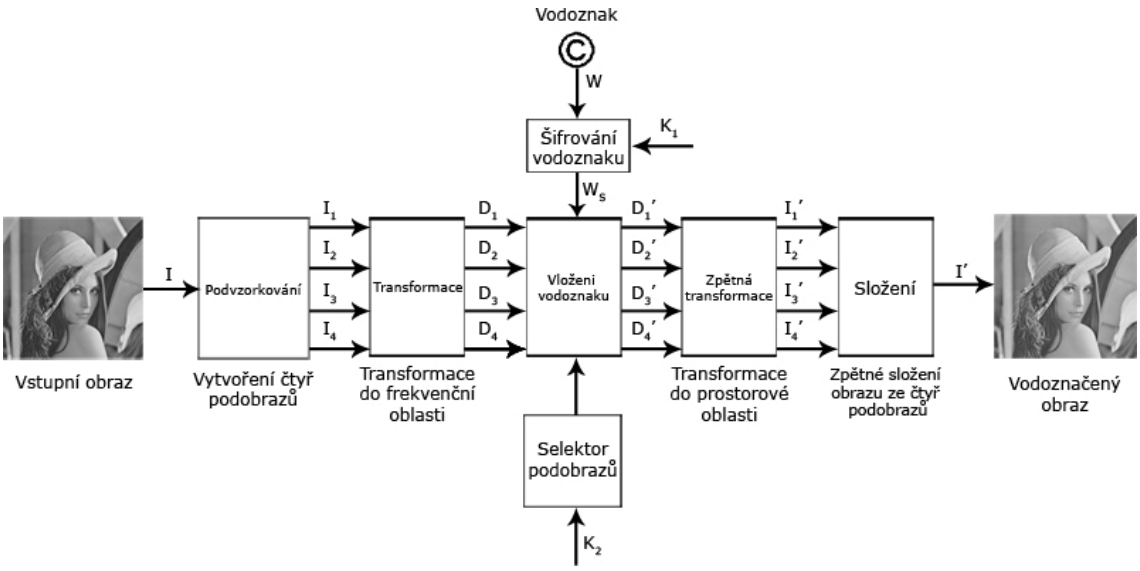
U geometrických útoků bylo vytažení vodoznaku téměř vždy neúspěšné, vytažený vodoznak se až na malé výjimky neshodoval se svým originálem. Hodnota *NCC* se pohybovala v rozmezí 0,4 až 0,6. Mezi geometrické útoky patří oříznutí obrazu, deformace, rotace,posun, projektivní transformace, odstranění řádku, sloupce atd.

U této metody vodoznačení vidím hlavní nedostatek v absenci tajného klíče, který by vybíral oblasti (jednotlivé bloky) vložení vodoznaku. To je také důvodem neúspěchu odolnosti této metody při geometrických útocích, jako je oříznutí obrazu, protože vodoznak je vložen do pevně stanovených bloků u horního okraje obrazu. Pokud útočník ví, že se vodoznak nachází v těchto místech, je už pro něj snadné odstranit značnou, úplnou část vložené tajné informace.

3.2. Realizace druhé metody

Tato část kapitoly popisuje druhou realizaci metody popsanou v literatuře [10]. Jde o poměrně novou metodu vkládání vodoznaku. Je založená na vytvoření čtyř podobrazů z původního obrazu pomocí podvzorkovaní. K vodoznačení se využívá vždy dvou podobrazů zvolených podle klíče. Jak už bylo naznačeno, hlavním rozdílem v zabezpečení vodoznačení oproti předchozí metodě, je v použití dvou tajných klíčů. Metodu můžeme zařadit do skupiny poloprivátních systému zabezpečení vodoznaků, protože při vytažení vodoznaku je vyžadována znalost tajných klíčů a originálního vodoznaku.

3.2.1. Vložení vodoznaku do obrazu



Obr. 3.11: Znázornění principu vložení vodoznaku

Proces vodoznačení je znázorněn na obrázku 3.11. Vstupní obraz v odstínech šedi byl k účelu zabezpečení použit obraz Lenny (512 × 512 pix, 8 bit) jako u předchozí metody. Originální obraz je rozdělen na čtyři dílčí podobrazy pomocí podvzorkovaní. Z nechráněné obrazové informace o velikosti $M \times N$ jsou odebírány vzorky dat v bloku podvzorkování podle následující úvahy [10]:

$$I_1(i,j) = I(2i,2j),\ I_2(i,j) = I(2i,2j+1),\ I_3(i,j) = I(2i+1,2j),\ I_4(i,j) = I(2i+1,2j+1), \qquad (3.5)$$

kde I je originální obraz, $I_{1\text{-}4}$ jsou jednotlivé dílčí podobrazy, i = 0,1,2…M/2-1, j = 0,1,2…N/2-1.

Pro lepší názornost jsou v tab. 6 zobrazeny jednotlivé odebírané vzorky z originálního obrazu o velikosti 8 × 8.

Tab. 6: Znázornění odebírání vzorků do dílčích podobrazů

	0	1	2	3	4	5	6	7
0	I_1	I_2	I_1	I_2	I_1	I_2	I_1	I_2
1	I_3	I_4	I_3	I_4	I_3	I_4	I_3	I_4
2	I_1	I_2	I_1	I_2	I_1	I_2	I_1	I_2
3	I_3	I_4	I_3	I_4	I_3	I_4	I_3	I_4
4	I_1	I_2	I_1	I_2	I_1	I_2	I_1	I_2
5	I_3	I_4	I_3	I_4	I_3	I_4	I_3	I_4
6	I_1	I_2	I_1	I_2	I_1	I_2	I_1	I_2
7	I_3	I_4	I_3	I_4	I_3	I_4	I_3	I_4

Následně je každý z podobrazů $I_{1\text{-}4}$ převeden do frekvenční oblasti, bez dalšího rozkladu na jednotlivé bloky, pomocí diskrétní kosinové transformace (DCT). Proces transformace pomocí 2D-DCT je popsán v předchozí metodě vodoznačení.

Na vstup vodoznačení přichází binární obraz vodoznaku v šifrované podobě. Šifrování je možno popsat následovně:

$$W_S = E_S\,(W, K_1), \qquad (3.6)$$

kde jako šifrovací funkci E_S jsem zvolil logickou funkci XOR.

Tab. 7: Pravdivostní tabulka logické funkce XOR

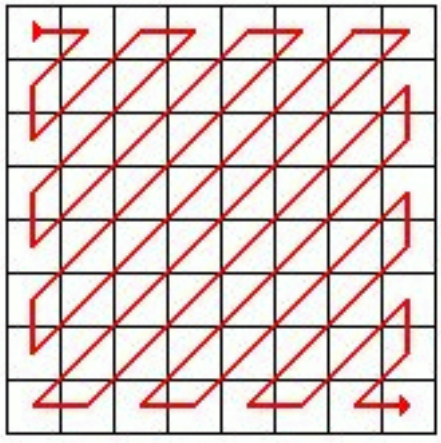
W	K_1	W_S
0	0	0
0	1	1
1	0	1
1	1	0

Smysluplný význam vodoznaku je tímto způsobem v utajení. Jedná se o symetrický kryptografický systém, protože pro šifrování a dešifrování je použit stejný klíč K_1. Zašifrovaný kryptogram je možné rozluštit metodou zkoušení tzv. hrubou silou (*brute force*). Při zkoušení nesprávného klíče získá útočník změť nesmyslných znaků (obr. 3.12d).

a) b) c) d)

Obr. 3.12 vodoznak: a) ordinální b) klíč K_1 vodoznaku c) zašifrovaný vodoznak d) dešifrovaný vodoznak s použitím špatného klíče

Další část vstupující do bloku vodoznačení je selektor podobrazů. Podle klíče K_2 se vybírají vždy dva dílčí podobrazy ze čtyř. Z těchto dvou podobrazů jsou vyčítány DCT koeficienty zig-zag čtením stejně jako u standardu JPEG (obr 3.13).



Obr. 3.13: Vyčítání zig-zag z matice 8 × 8

Vyčítání začíná od stejnosměrné složky, přes nízkofrekvenční oblast až k pásmu vysokých frekvencí.

Algoritmus vložení vodoznaku je založen na porovnávání velikostí frekvenčních složek. Pro každý bit vodoznaku jsou na výběr čtyři dílčí podobrazy $D_{1\text{-}4}$. Podle klíče $K_2 \in \{i, j\}$ jsou vybírány náhodně vždy dva dílčí podobrazy tak, že $i, j \in \{1,2,3,4\}$, kde $i \neq j$. Uvažujme m-tý bit vodoznaku W_S, který je vložen do m-tého páru frekvenčních koeficientů v pořadí zig-zag čtení, kde se neuvažují stejnosměrné složky. Jestliže na vstupu bloku vodoznačení je m-tá hodnota vodoznaku W_S rovná „1“ a m-tý pár DCT koeficientů (označme V_a , V_b) odpovídá tomu, že $V_a < V_b$, pak je potřeba přehodit i a j v klíči K_2. Pokud je však hodnota vodoznaku „0“ a $V_a > V_b$, dojde k záměně i a j v K_2. Ve zjednodušení může napsat:

Vstupní hodnota vodoznaku $W = 0$, $V_a < V_b \rightarrow K_2 \{i, j\}$,
$V_a > V_b \rightarrow K_2 \{j, i\}$.

Vstupní hodnota vodoznaku $W = 1$, $V_a > V_b \rightarrow K_2 \{i, j\}$,
$V_a < V_b \rightarrow K_2 \{j, i\}$.

Na rozdíl od předchozí metody, kde se mezi sebou přímo vyměňovaly jednotlivé frekvenční koeficienty, tady dochází pouze k záměně pořadí zvolených dílčích podobrazů v klíči K_2. To má za následek vyšší hodnotu nevnímatelnosti vodoznaku v obraze.

Odolnost vodoznaku v obraze se nastavuje podle parametru k. Nejdříve se vypočítá:

$$D_1 = \frac{|V_a| + |V_b|}{2}, \tag{3.7}$$

$$D_2 = \frac{V_a - V_b}{2}. \tag{3.8}$$

Určí se hodnota poměru D_1 a D_2 následovně:

$$\left|\frac{D_2}{D_1}\right| \leq \beta, \tag{3.9}$$

kde β je hodnota nastaveného prahu.

Jestliže je splněna nerovnost (3.9) upraví se hodnoty frekvenčních koeficientů:

$$V_a' = V_a + k(2W_m - 1)D_1, \tag{3.10}$$

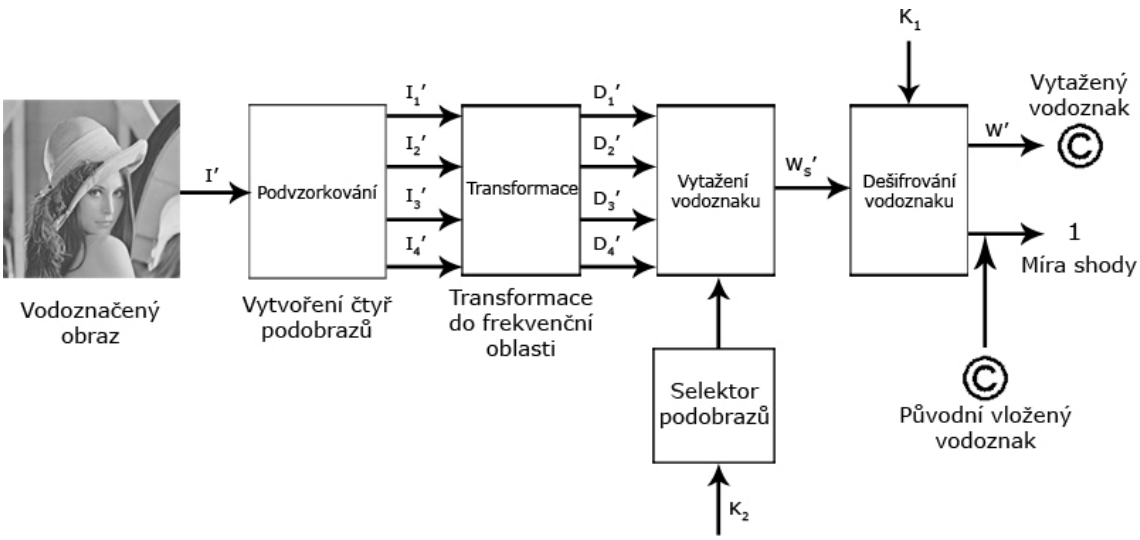
$$V_b' = V_b - k(2W_m - 1)D_1, \tag{3.11}$$

kde W_m je m-tá hodnota zašifrovaného vodoznaku.

V případě nesplněné podmínky nerovnosti (3.9) se ponechají koeficienty bez modifikací.

K získání chráněné obrazové informace je potřeba převod z frekvenční oblasti zpět do prostorové zpětnou diskrétní kosinovou transformací a posléze složení jednotlivých dílčích podobrazů v jeden výsledný obraz (viz. obr. 3.11).

3.2.2. Vytažení vodoznaku z obrazu



Obr. 3.14: Znázornění vytažení vodoznaku

Realizace vytažení tajné informace je blokově znázorněna na obrázku 3.14. K samotnému vytažení vodoznaku je potřeba dvou vstupních parametrů, kterými jsou vodoznačný obraz a klíč selekce podobrazů K_2. Výstupem je vodoznak v zašifrované formě. Klíčem K_1 dešifrujeme a získáme tak informaci o vytaženém vodoznaku, který je v ideálním případě stejný jako vložený originál (hodnota $NCC = 1$).

Mějme čtyři dílčí podobrazy $D_{1\text{-}4}$' převedené do frekvenční oblasti. Vytažení vodoznaku spočívá v porovnávání páru frekvenčních koeficientů v pořadí zig-zag u jednotlivých zvolených podobrazů podle klíče K_2. Pokud je první koeficient z páru *m*-tého pořadí větší nebo roven druhému, zapíše se do výstupního pole vytaženého vodoznaku hodnota „1"-bílá. Jestliže tomu tak není, zapíše se „0"-černá. Můžeme napsat:

$$V_a \geq V_b \rightarrow \text{výstup „1"}$$
$$V_a < V_b \rightarrow \text{výstup „0"}$$

Takto vytaženou informaci o vloženém vodoznaku je ještě potřeba dešifrovat klíčem K_1. Tím získáme vodoznak *W'*.

3.2.3. Test odolnosti metody

K simulaci útoků na chráněná obrazová data byl použit aplikační nástroj Checkmark. K vodoznační byl použit stejný vstupní obraz a stejný vodoznak jako v předchozí metodě. Výstup vodoznační je vidět na obrázku 3.15b. Robustnost vodoznaku byla nastavena na hodnotu $k = 0.1$ a hodnota prahu $\beta = 4$ (viz. rov 3.9-3.11).

a)

b)

c)

Obr. 3.15. Lenna: a) nechráněný obraz, b) vodoznačený obraz s *PSNR* = 34,13 dB, c) vložený vodoznak

Hranice rozpoznatelnosti vodoznaku se svým originálem je pro srovnání stejná jako u předchozí metody (*NCC* = 0.79). Vytažený vodoznak je považován za shodný se svým originálem, pokud hodnota *NCC* je větší nebo rovna hodnotě 0,79. V opačném případě je vytažený vodoznak považován za neshodný.

Útok kompresí JPEG:

Tab. 8: Hodnoty testu odolnosti po kompresi JPEG

Stupeň kvality JPEG *Q* [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
100	1	1
90	0,965	1
85	0,935	1
80	0,898	1
75	0,895	1
60	0,834	1
50	0,814	1
40	0,811	1
30	0,824	1
25	0,849	1
15	0,833	1
10	0,814	1

Vložený vodoznak byl zcela odolný proti kompresi JPEG (tab. 8). Na obrázcích 3.16c a 3.16d jsou zobrazeny vytažené vodoznaky se stupněm kvality JPEG komprese $Q = 75$ a $Q = 10$.

a)

b)

c)

d)

Obr. 3.16. Útok kompresí JPEG: a) Q=75, b) Q=10, c) vytažený vodoznak pro Q=75, d) vytažený vodoznak pro Q=10

Útok vlnkovou kompresí:

Tab. 9: Hodnoty testu odolnosti po vlnkové kompresi

Kompresní poměr [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
1:1	0,999	1
1:2	0,999	1
1:5	0,968	1
1:10	0,909	1
1:13	0,886	1
1:16	0,873	1
1:20	0,859	1
1:26	0,842	1
1:40	0,831	1
1:80	0,828	1

a)

b)

c)

d)

Obr. 3.17. Útok vlnkovou kompresí: a)komprese1:5, b)komprese1:40, c) vytažený vodoznak z komprese 1:5, d) Vytažený vodoznak z komprese 1:40

Proti útokům kompresí byla metoda vodoznačení velmi dobře odolná. V tabulce 9 jsou výsledky vytažení vodoznaku po útoku vlnkovou kompresí a k tomu odpovídající obrázky 3.17.

Útoky založené na filtrování obsahu:

Tab. 10: Hodnoty testu odolnosti po filtraci obsahu

Filtr	Velikost filtrovacího okna [pixel]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
Gaussovské rozostření	3×3	0,987	1
Gaussovské rozostření	5×5	0,987	1
Zostření	3×3	0,965	1

Obr. 3.18. Útok filtrováním obsahu: a)rozostření - filt. okno 5×5 pix.,b)zostřením, c)vytažený vodoznak z rozostření-filt.okno 5×5 pix., d)vytažený vodoznak po útoku zostřením

Realizovaná metoda, stejně jako předchozí, byla zcela odolná proti útokům založených na filtraci v obraze, jak je z tab. 10 a obrázků a obrázků 3.18 patrné.

Útoky založené na převzorkování obrazového signálu:

Tab. 11: Hodnoty testu odolnosti po převzorkování obrazového signálu

Typ [-]	Míra podvzorkování [-]	Míra nadvzorkování [-]	Normalizovaná vzájemná korelace *NCC* [-]	Shodnost vodoznaků (1-ANO, 0-NE)
1	0,75	1,33	0,916	1
2	0,5	2	0,493	0
3	0,75	1,3	0,73	0
4	0,5	1,9	0,705	0

a) b)

c) d)

Obr. 3.19 Útok převzorkováním: a) vodoznačný obraz po převzorkování typu 1, b) vodoznačný obraz po převzorkování typu 4, c)vytažený vodoznak po převzorkování typu 1, d) vytažený vodoznak po převzorkování typu 4

Útok převzorkování typu 1 nezmodifikoval vložený vodoznak do takové míry, aby se stal po algoritmu detekce nečitelným (tab. 11, obr. 3.10c). Detekce vodoznaku byla u převzorkování typu 3 a 4 neúspěšná.

Výhodou metody je rovnoměrné rozložení vodoznaku v celém obraze pomocí podvzorkování. Takto vložený vodoznak se dá velice obtížně odstranit z celé obrazové informace. Další výhodu bych uvedl v použití dvou tajných klíčů.

U této metody vodoznačení vidím nevýhodu v tom, pokud máme rozměrově větší vodoznak, může dojít k tomu, že se při vodoznačení v transformační oblasti dostaneme do oblasti vysokých frekvencí. Důvodem je, že vodoznačení neprobíhá v pevně zvolené frekvenční oblasti, ale v pořadí zig-zag vyčítání koeficientů. V této oblasti se stává vložený vodoznak málo odolný proti různým modifikacím obrazu.

Všechny výsledky testů odolnosti vložených vodoznaků jsou pro svůj značný rozsah umístěny na přiloženém CD.

ZÁVĚR

V diplomové jsem se seznámil s problematikou zabezpečení obrazových dat pomocí vložení vodoznaku. Prostudoval jsem techniky vložení vodoznaku a zrealizoval dvě metody vodoznačení ve frekvenční oblasti. Tato technika vkládání vodoznaku je zvolena pro její dobrou odolnost proti obrazovým kompresím. Metody pracující v transformační oblasti jsou v dnešní době nejvyužívanějšími metodami vodoznačení v obraze. Základem zrealizovaných metod je diskrétní kosinová transformace (DCT). K testování odolnosti vložených vodoznaků je použito aplikačního nástroje Checkmark.

První metoda je založená na záměně vybraných koeficientů. Odolnost vodoznaku jsem zvolil s ohledem na jeho nevnímatelnost v obraze. Výsledky testů jsou uvedeny a zhodnoceny v kapitole 3.3. Metoda má nedostatky hlavně při útocích, jako je oříznutí obrazu, protože vodoznak je vložen do pevně stanovených bloků u horního okraje obrazu. Pokud útočník ví, že se vodoznak nachází v těchto místech, je už pro něj snadné odstranit značnou část vložené tajné informace.

Druhá metoda je založená na vytvoření čtyř podobrazů z původního obrazu pomocí podvzorkovaní. K vodoznačení se využívá vždy dvou podobrazů zvolených podle tajného klíče. Hlavní rozdíl v zabezpečení algoritmu vodoznačení oproti předchozí metodě je v použití dvou tajných klíčů. Nevýhoda metody je v použití rozměrově větších vodoznaků vzhledem k celkovému rozměru obrazu, kdy může dojít k tomu, že se při vodoznačení v transformační oblasti dostaneme do oblasti vysokých frekvencí. V této oblasti se stává vložený vodoznak málo odolný proti různým modifikacím obrazu.

POUŽITÁ LITERATURA

[1] PAN, J.S., HUANG, H.CH., JAIN, L.C. *Inteligent Watermarking* Techniques, London: World Scientific Publishing, 2004. 639 s. ISBN 981-238-955-5

[2] LEVICKÝ, D. *Multimediálne Telekomunikáci: Multimedia, Technologie a Vodoznaky*, Košice: Elfa, 2002, 240 s. ISBN 80-89066-58-5

[3] VRBA, K., NAGY, Z. *Multimediální Služby*, Brno: elektronický text, 81 s. Dostupné z URL: <https://www.feec.vutbr.cz/et/skripta/utko/Multimedialni_sluby_S.pdf>

[4] HOŠEK, J.*Vodoznačení Video Obsahu*, Elektrorevue. 2007, 20 s. ISBN 1213-1539

[5] ČÍKA, P. *Přednášky z předmětu Multimédia*, Brno: elektronický text

[6] ČÍKA, P. *New watermarking scheme for colour image*, Brno: elektronický text, 8 s.

[7] SEITZ, CH. *Digital Watermarking foe Digital Media*, London: Information Science Publishing. 2005. 262 s. ISBN 1-59140-518-1

[8] SHI, Y. Q., SUN, H. *Image and Video Compression for Multimedia Engineering: fundamentals, algorithms, and standards*, USA: CRC Press LCC, 2000. 462 s. ISBN 0-8493-3491-8

[9] SALEH, H.I., ELHADEDY, M.E., ASHOUR, M.A, ABOELSAUD, M.A. *Comparisons of DCT-Based and DWT-Based Watermarking Techniques*, Egypt: elektronický text, 5 s. Dostupné z URL: <http://icbmp.uaeu.ac.ae/Proceedings/PDFPAPERS/27_ICBMP.pdf>

[10] WEI, L., HONGTAO, L., FU-LAI, CH. *Robust digital image watermarking based on subsampling*, China: elektronický text, 8 s. Dostupné z URL: <http://orfeo.unipv.it/cdol/tesine06_07/watermarking10.pdf>

OBSAH CD

Adresářová struktura na CD je následující:

- adresář *text* – obsahuje text diplomové práce
    - adresář *pdf* – text této práce ve formátu *pdf*
    - adresář *obr* – všechny obrázky v této práci
- adresář *metody* – obsahuje vytvořené metody v prostředí MATLAB
    - adresář *1* – obsahuje skripty první metody (přípona **.m*)
    - adresář *2* – obsahuje skripty druhé metody (přípona **.m*)
- adresář *test* – obsahuje výstup z aplikačního nástroje Checkmark
    - adresář *1* – obsahuje výstup testu první metody (přípona **.html*)
    - adresář *2* – obsahuje výstup testu druhé metody (přípona **.html*)
- adresář *obrazky* – obsahuje testovací obraz a vodoznak (přípona **.bmp*)